

UNITED STATES DISTRICT COURT
DISTRICT OF WESTERN OF MISSOURI

JOHN ALEXANDER and Case No. 4:17-cv-788
RODNEY WILLIAMS,
(Missouri) consumers, individually CLASS ACTION
and on behalf of all others, ALLEGATION COMPLAINT

Plaintiffs, Negligence

v. 28 U.S.C. § 1332

EQUIFAX INC., Demand for Jury Trial

Defendant.

CLASS ACTION COMPLAINT

Plaintiffs John Alexander and Rodney Williams, individually and on behalf of the classes defined below, bring this Class Action Complaint (“Complaint”) against Equifax, Inc. and Equifax Workforce Solutions, Inc. a/k/a TALX Corporation (collectively, “Equifax” or “Defendants”), and allege as follows:

THE PARTIES

1. Equifax Inc. (Equifax) is a multi-billion dollar Georgia corporation that provides credit information services to millions of businesses, governmental units, and consumers across the globe. Equifax operates through various subsidiaries including Equifax Information Services, LLC, and Equifax Consumer Services, LLC aka Equifax Personal Solutions aka PSOL. Each of these entities acted as agents of Equifax or in the alternative, acted in concert with Equifax as alleged in this complaint.
2. Equifax is one of the major credit reporting agencies in the United States. As a

credit bureau service, Equifax is engaged in a number of credit-related services. In conjunction therewith, Equifax maintains information related to the credit history of consumers and provides the information to credit grantors who are considering a borrower's application for credit or who have extended credit to the borrower.

3. John Alexander is an individual consumer residing in the Kansas City, Missouri, area and Rodney Williams is an individual consumer residing in the Kansas City, Missouri, area. On or around September 7, 2017, Plaintiffs received notification that their personal information was the subject of an Equifax data breach. As a result of the data breach and the substantial risk of identity theft, Plaintiffs enrolled in identity theft protections services at a cost to him.

NATURE OF THE CASE

4. On September 7, 2017, Equifax advised the general public that information that it collected on behalf of over 143 million consumers was the subject of a data breach, in which unauthorized individuals accessed the personal and credit information of those individuals.

5. The data breach occurred because Equifax failed to implement adequate security measures to safeguard consumers' data and willfully ignored known weaknesses in its data security, including its information systems. Unauthorized parties routinely attempt to gain access to and steal personal information from networks and information systems—entities such as Equifax, which is known to possess a significant number of valuable personal and financial information.

6. Armed with this personal information, identity thieves can commit a variety of

crimes that harm victims of the data breach. For example, such criminals can take out loans, mortgage property, open financial accounts, and open credit cards in a victim's name; use a victim's information to obtain government benefits or file fraudulent returns to obtain a tax refund; obtain a driver's license or identification card in a victim's name; gain employment in a victim's name; obtain medical services in a victim's name; or give false information to police during an arrest. In addition, hackers also routinely sell victims' information to other individuals who intend to misuse the information.

7. As a result of Equifax's willful failure to prevent the data breach, Plaintiffs and Class Members have been exposed to fraud, identity theft, and financial harm, as detailed below, and to a substantial, heightened, and imminent risk of such harm in the future. It cannot be questioned that the private information of Plaintiffs and Class Members was taken for the purpose of stealing the identity of Plaintiffs and Class Members which has already resulted in and will continue to result in damage to them. Plaintiffs and Class Members have to monitor their financial accounts and credit histories more closely and frequently to guard against identity theft. Plaintiffs and Class Members also have incurred, and will continue to incur, additional out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures in order to detect, protect, and repair the data breach's impact on their private information for the remainder of their lives. Going forward, Plaintiffs and Class Members anticipate spending considerable time and money for the rest of their lives in order to detect and respond to the impact of the data breach.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over this action under the Class Action

Fairness Act, 28 U.S.C. § 1332(d) because this is a class action involving more than 100 Class Members who are citizens of different states. In addition, the amount in controversy exceeds \$68 billion exclusive of interest, costs and penalties.

9. This Court has personal jurisdiction over Defendant under 28 U.S.C. § 1391 because the bulk of Missouri consumers with credit and personal information stored by Equifax live in the Kansas City, Missouri, area. Further, Equifax has availed itself to this jurisdiction as it regularly transacts business in this District and a substantial part of the events, acts and omissions giving rise to Plaintiffs' claims occurred in this District.

FACTUAL ALLEGATIONS

10. Plaintiffs file this complaint as a national class action on behalf of over 143 million consumers across the Country harmed by Equifax's failure to adequately protect their credit and personal information. This complaint requests Equifax provide fair compensation in an amount that will ensure every consumer harmed by its data breach will not be out-of-pocket for the costs of independent third-party credit repair and monitoring services. This Complaint's allegations are based on personal knowledge as to Plaintiffs' conduct and made on information and belief as to the acts of others.

11. Equifax is one of the major credit reporting agencies in the United States. As a credit bureau service, Equifax is engaged in a number of credit-related services, including providing services. Throughout the past year, Equifax collected and stored personal and credit information from John Alexander and Rodney Williams, including their social security numbers, birth dates, home addresses, driver's license information, and credit card numbers.

12. Equifax touts itself as an industry leader in data breach security and often promotes the importance of data breach prevention. Equifax offers services directly targeted to assisting businesses who have encountered a data breach. Equifax, through its marketing of its services, promised its customers that it would reasonably protect the privacy and confidentiality of personal information about consumers.

13. Equifax owed a legal duty to consumers like John Alexander and Rodney Williams to use reasonable care to protect their credit and personal information from unauthorized access by third parties. Equifax knew that its failure to protect John Alexander and Rodney Williams' credit and personal information from unauthorized access would cause serious risks of credit harm and identify theft for years to come.

14. On September 7, 2017, Equifax announced for the first time that from May to July 2017, its database storing John Alexander and Rodney Williams' credit and personal information had been hacked by unauthorized third parties, subjecting John Alexander and Rodney Williams to credit harm and identify theft.

15. In an attempt to increase profits, Equifax negligently failed to maintain adequate technological safeguards to protect John Alexander and Rodney Williams' information from unauthorized access by hackers.

16. Equifax knew and should have known that failure to maintain adequate technological safeguards would eventually result in a massive data breach. Equifax could have and should have substantially increased the amount of money it spent to protect against cyber-attacks but chose not to. Consumers like John Alexander and Rodney Williams should not have to bear the expense caused by Equifax's negligent failure to safeguard their credit and personal information from cyber-attackers.

17. As a result of the compromising of their personal information, Plaintiffs and Class Members have experienced and will face a substantial risk of experiencing the following injuries:

- money and time expended to prevent, monitor, detect, contest, and repair identity theft, fraud, and/or other unauthorized uses of personal information;
- money and time lost as a result of fraudulent access to and use of their financial accounts;
- loss of use of and access to their financial accounts and/or credit;
- money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;
- impairment of their credit scores, ability to borrow, and/or ability to obtain credit;
- lowered credit scores resulting from credit inquiries following fraudulent activities;
- money, including fees charged in some states, and time spent placing fraud alerts and security freezes on their credit records;
- costs and lost time obtaining credit reports in order to monitor their credit records;
- costs of credit monitoring, as Defendant has offered none to date;
- costs and lost time from dealing with administrative consequences of the
- data breach, including by identifying, disputing, and seeking reimbursement for fraudulent activity, canceling compromised financial accounts and associated payment cards, and investigating options for credit monitoring and identity theft protection services;

- money and time expended to ameliorate the consequences of the filing of fraudulent tax returns;
- lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the data breach, including but not limited to efforts to research how to prevent, detect, contest, and recover from misuse of their personal information;
- loss of the opportunity to control how their personal information is used; and
- continuing risks to their personal information, which remains subject to further harmful exposure and theft as long as Equifax fails to undertake appropriate, legally required steps to protect the personal information in its possession.

18. The risks that Plaintiffs and Class Members bear as a result of the data breach cannot be fully mitigated by credit monitoring because it can only help detect, but will not prevent, the fraudulent use of Plaintiffs' and Class Members' private information. Instead, Plaintiffs and Class Members will need to spend time and money to protect themselves. For instance, credit reporting agencies impose fees for credit freezes in certain states. In addition, while credit reporting agencies offer consumers one free credit report per year, consumers who request more than one credit report per year from the same credit reporting agency (such as Equifax) must pay a fee for the additional report. Such fees constitute out-of-pocket costs to Plaintiffs and Class Members.

19. As a direct result of Equifax's negligence as alleged in this complaint, John Alexander and Rodney Williams suffered injury of loss to pay for third-party credit monitoring services he otherwise would not have had to pay. John Alexander and Rodney Williams hope Equifax will use this massive data breach, and their subsequent lawsuit, as

a teachable moment to finally adopt adequate safeguards to protect against this type of cyber-attack in the future.

20. Further, under the Gramm-Leach-Bliley Act (“GLBA”), Equifax was required to investigate and provide timely adequate notification of the data breach under federal regulations.

21. The Gramm-Leach-Bliley Act (“GLBA”) imposes upon “financial institutions” “an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information.” 15 U.S.C. § 6801. In accordance with 15 U.S.C. § 6801(b), to satisfy this obligation, financial institutions must satisfy certain standards relating to administrative, technical, and physical safeguards:

- a) to insure the security and confidentiality of customer records and information;
- b) to protect against any anticipated threats or hazards to the security or integrity of such records; and
- c) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

In order to satisfy their obligations under the GLBA, financial institutions must “develop, implement, and maintain a comprehensive information security program that is [1] written in one or more readily accessible parts and [2] contains administrative, technical, and physical safeguards that are appropriate to [their] size and complexity, the nature and scope of [their] activities, and the sensitivity of any customer information at issue.” See 16 C.F.R. § 314.4.

22. Upon information and belief, Equifax failed to “develop, implement, and maintain

a comprehensive information security program” with “administrative, technical, and physical safeguards” that were “appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue.” This includes, but is not limited to, Equifax’s failure to implement and maintain adequate data security practices to safeguard Class Members’ personal information; (b) failing to detect the data breach in a timely manner; and (c) failing to disclose that Defendants’ data security practices were inadequate to safeguard Class Members’ personal information.

23. Upon information and belief, Equifax also failed to develop and implement a risk-based response program to address incidents of unauthorized access to customer information in customer information systems as mandated by the GLBA. This includes, but is not limited to, Equifax’s failure to notify appropriate regulatory agencies, law enforcement, and the affected individuals themselves of the data breach in a timely and adequate manner.

24. Equifax has also failed to notify affected customers as soon as possible after it became aware of unauthorized access to sensitive customer information, and has failed to communicate directly with Class Members to date.

In addition, according to the FTC, the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data constitutes an unfair act or practices prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

By failing to have reasonable data security measures in place, Equifax engaged in an unfair act or practice within the meaning of Section 5 of the FTC Act.

Plaintiffs file this complaint as a national class action lawsuit.

CLASS ALLEGATIONS

25. The Missouri class consists of Missouri consumers who:

- a. Had personal or credit data collected and stored by Equifax,
and
- b. Who were subject to risk of data loss and credit harm and identity theft or had
to pay for third-party credit monitoring services as a result of Equifax's
negligent data breach from May to July 2017.

26. Excluded from the class are all attorneys for the class, officers and members of Equifax, including officers and members of any entity with an ownership interest in Equifax, any judge who sits on the case, and all jurors and alternate jurors who sit on the case.

27. The exact number of aggrieved consumers in Missouri can be determined based on Equifax's consumer database, estimated at 2,860,000 consumers – about half the population of Missouri.

28. Every aggrieved Missouri consumer suffered injuries as alleged in this complaint directly and proximately caused by Equifax's negligent failure to adequately protect its database from unauthorized access by third-party hackers.

29. The class is so numerous that joinder is impracticable. Upon information and belief, the Missouri class alone includes millions of consumers based on Equifax's estimate that its data breach affected 143 million consumers nationwide.

30. Common questions of fact and law predominate over any questions affecting only individual Class Members.

31. Common questions include whether Plaintiffs and the Missouri Class Members are entitled to equitable relief, whether Equifax acted negligently, and whether plaintiffs

and the Missouri Class Members are entitled to recover money damages.

32. Plaintiffs' claims are typical of the claims of the Missouri class because each suffered risk of loss and credit harm and identity theft caused by Equifax's negligent failure to safeguard their data, the injuries suffered by Plaintiffs and the Missouri Class Members are identical (i.e. the costs to monitor and repair their credit through a third-party service for at least 24 months), and plaintiffs' claims for relief are based upon the same legal theories as are the claims of the other Class Members. Plaintiffs will fairly and adequately protect and represent the interests of the class because their claims are typical of the claims of the Missouri class, they are represented by nationally known and locally respected attorneys who have experience handling class action litigation and consumer protection cases who are qualified and competent, and who will vigorously prosecute this litigation, and their interests are not antagonistic or in conflict with the interests of the Missouri class.

33. A class action is superior to other methods for fair and efficient adjudication of this case because common questions of law and fact predominate over other factors affecting only individual members, as far as Plaintiffs know, no class action that purports to include Missouri consumers suffering the same injury has been commenced in Missouri, individual Class Members have little interest in controlling the litigation, due to the high cost of actions, the relatively small amounts of damages, and because plaintiffs and their attorneys will vigorously pursue the claims. The forum is desirable because the bulk of consumers in Missouri who suffered injury caused by Equifax's negligence reside in the Kansas City, Missouri, metropolitan area. A class action will be an efficient method of adjudicating the claims of the Class Members who have suffered relatively

small damages, as a result of the same conduct by Equifax. In the aggregate, Class Members have claims for relief that are significant in scope relative to the expense of litigation.

34. The availability of Defendant's consumer data will facilitate proof of class claims, processing class claims, and distributions of any recoveries.

CAUSE OF ACTION

COUNT I

NEGLIGENCE

(On Behalf of the nationwide Class and the Statewide Subclass)

35. Plaintiffs hereby incorporate by reference all preceding paragraphs as if fully set forth herein.

36. Equifax owed a duty to Plaintiffs and Class Members, arising from the sensitivity of the information and the foreseeability of its data safety shortcomings resulting in an intrusion, to exercise reasonable care in safeguarding their sensitive personal information. This duty included, among other things, designing, maintaining, monitoring, and testing Equifax's security systems, protocols, and practices to ensure that Class Members' information adequately secured from unauthorized access.

37. Equifax owed a duty to Class Members to implement intrusion detection processes that would detect a data breach in a timely manner.

38. Equifax also had a duty to delete any private information that was no longer needed to serve client needs.

39. Equifax owed a duty to disclose the material fact that its data security practices were inadequate to safeguard Class Members' private information.

40. Equifax also had independent duties under state laws that required Equifax to reasonably safeguard Plaintiffs' and Class Members' private information and promptly notify them about the data breach.

41. Equifax had a special relationship with Plaintiffs and Class Members from being entrusted with their private information, which provided an independent duty of care. Plaintiffs' and other Class Members' willingness to entrust Equifax with their private information was predicated on the understanding that Equifax would take adequate security precautions. Moreover, Equifax had the ability to protect its systems and the private information it stored on them from attack.

42. As alleged in this complaint, Equifax undertook care of credit and personal information belonging to Plaintiffs and the Missouri putative class, then breached its legal duty by failing to maintain adequate technological safeguards, falling below the standard of care in the technological industry, directly and proximately causing foreseeable risk of data loss and credit harm and identity theft and other economic losses, in amounts to be decided by the jury.

43. Equifax breached its duties by, among other things: (a) failing to implement and maintain adequate data security practices to safeguard Class Members' private information; (b) failing to detect the data breach in a timely manner; (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' private information; and (d) failing to provide adequate and timely notice of the breach.

44. But for Equifax's breach of its duties, Class Members' private information would not have been accessed by unauthorized individuals.

45. Further, Plaintiffs and Class Members were foreseeable victims of Equifax's inadequate data security practices. Equifax knew or should have known that a breach of its data security practices, particularly, as on information and belief, Equifax has had similar data breaches in recent years.

46. Equifax's negligent conduct provided a means for unauthorized intruders to obtain Plaintiffs' and the Nationwide Class Members' private information and consumer reports.

47. As a result of Equifax's willful failure to prevent the data breach, Plaintiffs and Class Members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' private information has also diminished the value of the private information.

48. The damages to Plaintiffs and the Class Members were a proximate and reasonably foreseeable result of Equifax's breach of its duties.

49. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

50. Plaintiffs and the Missouri class are entitled to equitable relief in the form of an accounting of exactly how their credit and personal information was accessed without authorization by third parties, restitution, and unless agreed upon by Equifax, an order to

preserve all documents and information (and electronically stored information) pertaining to this case.

COUNT II

NEGLIGENCE PER SE

(On Behalf of the nationwide Class and the Statewide Subclass)

51. Plaintiffs hereby incorporates by reference all preceding paragraphs as if fully set forth herein.

52. Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45 prohibits “unfair...practices in or affecting commerce” including, as interpreted and enforced by the Federal Trade Commission (“FTC”), the unfair act or practice by businesses such as Equifax of failing to use reasonable measures to protect private information.

53. Equifax violated Section 5 of the FTC Act by failing to use reasonable measures to protect private information and not complying with applicable industry standards. Equifax’s conduct was particularly unreasonable given the nature and amount of private information it obtained and stored and the foreseeable consequences of a data breach in their systems, including specifically the immense damages that would result to consumers.

54. Equifax’s violation of Section 5 of the FTC Act constitutes *negligence per se*.

55. Members of the Class and Subclass are within the class of persons Section 5 of the FTC Act was intended to protect as they are individuals engaged in trade and commerce, and bear the risk associated with defendant’s failure to properly secure their private information.

56. Moreover, the harm that has occurred is the type of harm the FTC Act was intended to guard against. The FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, have put consumers' personal data at unreasonable risk, causing the same harm suffered by Class Members and Subclass Members.

57. In addition, Equifax was further required under the Gramm-Leach-Bliley Act ("GLBA") to satisfy certain standards relating to administrative, technical, and physical safeguards:

- a) to insure the security and confidentiality of customer records and information;
- b) to protect against any anticipated threats or hazards to the security or integrity of such records; and
- c) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

58. Equifax violated GLBA by failing to "develop, implement, and maintain a comprehensive information security program" with "administrative, technical, and physical safeguards" that were "appropriate to [its] size and complexity, the nature and scope of [its] activities, and the sensitivity of any customer information at issue." This includes, but is not limited to, Equifax's failure to implement and maintain adequate data security practices to safeguard Class Members' personal information; (b) failing to detect the data breach in a timely manner; and (c) failing to disclose that Defendants' data security practices were inadequate to safeguard Class Members' personal information.

Plaintiffs and Class Members were foreseeable victims of Equifax's violations of the

FTC Act and GLBA. Equifax knew or should have known that its failure to take reasonable measures to prevent a breach of its data security systems, and failure to timely and adequately notify the appropriate regulatory authorities, law enforcement, and Class Members themselves would cause damages to Class Members.

59. Defendant's failure to comply with the applicable laws and regulations, including the FTC Act and GLBA, constitute negligence per se.

60. But for Equifax's violation of the applicable laws and regulations, Class Members' private information would not have been accessed by unauthorized individuals.

61. As a result of Equifax's willful failure to prevent the data breach, Plaintiffs and Class Members suffered injury, which includes but is not limited to exposure to a heightened, imminent risk of fraud, identity theft, and financial harm. Plaintiffs and Class Members must more closely monitor their financial accounts and credit histories to guard against identity theft. Class Members also have incurred, and will continue to incur on an indefinite basis, out-of-pocket costs for obtaining credit reports, credit freezes, credit monitoring services, and other protective measures to deter or detect identity theft. The unauthorized acquisition of Plaintiffs' and Class Members' private information has also diminished the value of the private information.

62. The damages to Plaintiffs and the Class Members were a proximate and reasonably foreseeable result of Equifax's breach of its duties.

63. Therefore, Plaintiffs and Class Members are entitled to damages in an amount to be proven at trial.

64. Plaintiffs and the Missouri class are entitled to equitable relief in the form of an

accounting of exactly how their credit and personal information was accessed without authorization by third parties, restitution, and unless agreed upon by Equifax, an order to preserve all documents and information (and electronically stored information) pertaining to this case.

COUNT III

WILLFUL VIOLATION OF THE FAIR CREDIT REPORTING ACT

65. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

66. The Fair Credit Reporting Act requires “consumer reporting agencies” to adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information, including appropriate measures to protect the confidentiality of such information 15 U.S.C. § 1681 *et seq.*

67. Under FCRA, a “consumer report” means any communication of information by a “consumer reporting agency” bearing on a customer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or collected as a factor in establishing eligibility for credit or insurance. 15 U.S.C. § 1681b.

68. Further, a “consumer reporting agency” means any person, which regularly engages in whole or in part the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties.

69. Plaintiffs and Class Members are “consumers” or “persons” under FCRA, 15 U.S.C. § 1681a.

70. Defendant is a “consumer reporting agency” under FCRA because it regularly engages in providing credit or other information on consumers to Atlas Premium Insurance Company for the purpose of determining whether to finance monthly installment premium payment plans.

71. Atlas admits on its website in the FAQs that it does not run credit checks on applicants and instead relies solely on the credit and other consumer information furnished to it by Defendant.

72. Defendant maintains “consumer reports” within the meaning of FCRA.

73. As a “consumer reporting agency,” Defendant is required to “maintain reasonable procedures” to limit the use of consumer reports, including reasonable and effective procedures to limit unauthorized access to Defendant’s databases. 15 U.S.C. § 1681e.

74. Defendant willfully breached its requirement under FCRA to protect its databases by choosing not to encrypt the Insurance Documents and allowing public access to them.

75. Under FCRA, Plaintiffs and Class Members are entitled to statutory damages of \$100 per person for violations of this duty, or actual damages if greater (to a maximum of \$1,000 per person), plus costs and attorney’s fees. 15 U.S.C. § 1681n.

COUNT IV
NEGLIGENT VIOLATION OF THE FAIR CREDIT REPORTING ACT
(Pled in the Alternative to Count III)

76. Plaintiffs incorporate the above allegations by reference as if set forth fully herein.

77. The Fair Credit Reporting act requires “consumer reporting agencies” to adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information, including appropriate measures to protect the

confidentiality of such information.

78. Under FCRA, a “consumer report” means any communication of information by a “consumer reporting agency” bearing on a customer’s credit worthiness, credit standint, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or collected as a factor in establishing eligibility for credit or insurance.

79. Further, a “consumer reporting agency” means any person which regularly engages in whole or in part the practice of assembling or evaluating consumer credit information or other consumers for the purpose of furnishing consumer reports to third parties.

80. Plaintiffs and Class Members are “consumers” or “persons” under FCRA.

81. Defendant is a “consumer reporting agency” under FCRA because it regularly engages in providing credit or other information on consumers to Atlas Premium Insurance Company for the purpose of determining whether to finance monthly installment premium payment plans.

82. Atlas admits on its website in the FAQs that it does not run credit checks on applicants and instead relies solely on the credit and other consumer information furnished to it by Defendant.

83. Defendant maintains “consumer reports” within the meaning of FCRA.

84. As a “consumer reporting agency” Defendant is required to “maintain reasonable procedures” to limit the use of consumer reports, including reasonable and effective procedures to limit unauthorized access to Defendant’s databases.

85. Defendant was negligent in failing to maintain reasonable procedures to protect its databases by choosing not to encrypt the Insurance Documents and allowing public

access to them.

86. Defendant's conduct violated FCRA and Plaintiffs and Class Members have been damaged by Defendant's conduct in an amount to be determined at trial.

87. Under FCRA, Plaintiffs and Class Members are statutorily entitled to recover actual damages plus costs and attorney's fees. 15 U.S.C. § 1681o.

PRAYER FOR RELIEF

Plaintiffs, on behalf of themselves and all others similarly situated, request that the Court enter judgment against Equifax as follows:

- a. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class and requested herein, appointing the undersigned as Class Counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;
- b. Unless agreed upon by Equifax, an order to preserve all documents and information (and electronically stored information) pertaining to this case;
- c. Judgment against Equifax for fair compensation in an amount to be decided by the jury, and costs,
- d. An order requiring Defendants to pay all costs associated with Class notice
- e. and administration of Class-wide relief;
- f. An award to Plaintiff and all Class Members of compensatory, consequential, incidental, and statutory damages, restitution, and disgorgement, in an amount to be determined at trial;
- g. An award to Plaintiffs and all Class Members of credit monitoring and identity theft protection services;

- h. An award of attorneys' fees, costs, and expenses, as provided by law or equity;
- i. An order Requiring Defendants to pay pre-judgment and post-judgment interest, as provided by law or equity;
- j. Such other or further relief as the Court deems necessary;
- k. Order the Defendant to remedy the data breach;
- l. Order an independent privacy audit of Defendant and related entities to determine whether similar data breaches are also occurring and to report to the Court the cause of the current data breach;
- m. Order the parties to confer on any recommended redactions to this complaint and preparation of a public version to be ECF-filed after the data breach has been remedied;
- n. Award contractual damages to Plaintiffs and the Class for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial, including interest thereon;
- o. Award restitution to Plaintiffs and the Class against Defendant;
- p. Award statutory damages under the Fair Credit Reporting Act;
- q. Permanently restrain Defendant and its officers, agents, employees and attorneys from violating the statutes referred to herein or otherwise violating its privacy policy with respect to data protection.

DEMAND FOR A JURY TRIAL

Plaintiffs request a trial by jury on all issues in this case which are so triable.

Respectfully submitted,

/s/Nimrod T. Chapel, Jr.

Nimrod T. Chapel, Jr. #MO46875
THE CHAPEL LAW GROUP, LLC
219 E. Dunklin, Suite A
Jefferson City, MO 65101
Phone: 573-634-8884
Fax: 573-635-6291
Email: nimrod@chapellaw.com

*/s/*Jason O. Barnes

Jason O. Barnes #MO57583
BARNES AND ASSOCIATES, LLC
219 E. Dunklin, Suite A
Jefferson City, MO 65101
Phone: 573-634-8884
Fax: 573-635-6291
Email: jaybarnes5@gmail.com

ATTORNEYS FOR PLAINTIFF